An Intuitionistic Formula Hierarchy Based on High-School Identities

Taus Brock-Nannestad, Danko Ilik

AN INTUITIONISTIC FORMULA HIERARCHY BASED ON HIGH-SCHOOL IDENTITIES

TAUS BROCK-NANNESTAD AND DANKO ILIK

Abstract. We revisit intuitionistic proof theory from the point of view of the formula isomorphisms arising from high-school identities. Using a representation of formulas as exponential polynomials, we first observe that invertible proof rules of sequent calculi for intuitionistic proposition logic correspond to equations using high-school identities, and that hence a so called high-school variant of a proof system can be obtained that is complete for provability, but contains no more than the non-invertible proof rules. We further show that, for proof calculi that do not include contraction, like the G4ip sequent calculus of Vorob'ev, Hudelmaier, and Dyckhoff, it may also be possible to interpret the non-invertible rules as strict inequalities between exponential polynomials. Finally, we extend the exponential polynomial analogy to first-order quantifiers, showing that it gives rise to a simple intuitionistic hierarchy of formulas, the first one that classifies formulas up to isomorphism, and proceeds along the same equivalences that lead to the classical arithmetical hierarchy.

1. Introduction

Classical logic has a standard semantics independent of the notion of proof. One could for instance do model theory without ever involving proof systems. For intuitionistic logic, however, the intended meaning of the logical connectives makes its semantics inherently proof-theoretic. For example, the intuitionistic validity of $F \vee G$ amounts to either having a proof of F or a proof of G.

Equivalence of formulas is perhaps also more subtle intuitionistically. First, whereas in classical first-order logic any formula can be characterized as belonging at an appropriate level of the arithmetical hierarchy through an equivalent formula in prenex form, in intuitionistic logic, the existence of an equally versatile hierarchy appears to be elusive (see Section 5). Second, the usual notion of equivalence which denotes implication in both directions is not semantics-, that is, proof-preserving: for instance, the equivalence $F \wedge F \leftrightarrow F$ only allows preserving proofs between the left-hand side and the right-hand side for some special cases of F. For instance, if F is a disjunction where each disjunct is provable. In this case, there would be four different possible proofs of the left-hand side, but only two different possible proofs of the right-hand side.

Isomorphism of formulas seems to be a better notion when our aim is to preserve semantics across an equivalence. This strong notion of equivalence of formulas,

$$F \cong G,$$

asks not only that $F \leftrightarrow G$, but also that there exist proof transformations ϕ and ψ, such that given any proof $\mathcal{D}_1$ of F and $\mathcal{D}_2$ of G, we have that

$$\psi(\phi(\mathcal{D}_1)) \equiv \mathcal{D}_1 \quad \text{and} \quad \phi(\psi(\mathcal{D}_2)) \equiv \mathcal{D}_2.$$

However, adopting isomorphism as the standard intuitionistic notion of equivalence makes us stumble upon another fundamental problem: having a good definition of *identity of proofs*, "$\equiv$", is itself open since the early days of intuitionistic proof theory (see [1] and Section 5).

For all of these reasons, the study of formal proof systems is perhaps more pressing for intuitionistic logic and constructive mathematics, than it is for classical mathematics. And, as constructive reasoning plays an important role in proof assistant software, these problems are also directly relevant to formal specification and verification of programs, not to mention the foundations of popular mathematical theories with intuitionistic cores, such as type theory and topos theory.

In this paper, we contribute to the intuitionistic proof theory related to the aforementioned problems by means of the fresh perspective of *intuitionistic formulas seen as exponential polynomials*.

In Section 2, we shall show that the invertible (i.e. asynchronous [2]) proof rules of G4ip [3], Vorob'ev, Hudelmaier, and Dyckhoff's sequent calculus for intuitionistic propositional logic, present simple isomorphisms that arise from high-school identities, and that hence one can build a so called high-school variant (HS) of G4ip, which is complete for provability, but does not need to contain invertible (i.e. asynchronous) proof rules. The calculus HS is thus the first proof system for intuitionistic logic that relies on the essential non-invertible (i.e. synchronous) rules only.

Furthermore, being a contraction-free variant of LJ, G4ip allows an interpretation of *non*-invertible rules as *in*-equalities between exponential polynomials. This is shown in Section 3, opening the possibility to use arithmetical or analytic arguments in intuitionistic proof theory: we give an application to termination of proof search.

In Section 4, we shall show how the analogy between formulas and exponential polynomials can be extended to the first-order quantifiers, obtaining a normal form for intuitionistic first-order formulas and a novel intuitionistic "arithmetical" hierarchy that preserves formula isomorphism, and hence identity of proofs. We believe that the proposed hierarchy can play a rôle similar to that of the arithmetical hierarchy for classical logic (which exists since the 1920s), as it is both simple and semantics-preserving.

Finally, Section 5 summarizes our results and discusses related work.

2. High-School Sequent Calculus

Identifying formulas of intuitionistic propositional logic with exponential polynomials – by writing $F \wedge G$ as FG, $F \vee G$ as $F+G$, $F \to G$ as G^F, and treating atomic formulas as variables – allows generalizing the notion of validity of equations in the standard model of positive natural numbers by the notion of formula isomorphism. Namely, if we take $F \cong G$ as defined in Section 1, the following implication holds (see [4] for a proof):

$$F \cong G \implies \mathbb{N}^+ \vDash F = G.$$

That is, if F and G are *isomorphic* intuitionistic formulas, then the corresponding arithmetical expressions must be *equal*, when the variables contained therein are interpreted as ranging over the positive natural numbers.

Reversing this implication poses interesting meta-theoretic problems (see [5, 6]). Nevertheless, we shall not need in this paper anything more than the isomorphisms

arising from the twelve high-school identities (HSI axioms):

$$F = F \tag{1}$$
$$F + G = G + F \tag{2}$$
$$(F + G) + H = F + (G + H) \tag{3}$$
$$FG = GF \tag{4}$$
$$(FG)H = F(GH) \tag{5}$$
$$F(G + H) = FG + FH \tag{6}$$
$$F1 = F \tag{7}$$
$$F^1 = F \tag{8}$$
$$1^F = 1 \tag{9}$$
$$F^{G+H} = F^G F^H \tag{10}$$
$$(FG)^H = F^H G^H \tag{11}$$
$$(F^G)^H = F^{GH}. \tag{12}$$

If we close these axioms under appropriate equality and congruence rules (see for instance [6]), we can talk about formal derivability of an equation, $\mathrm{HSI} \vdash F = G$, for which we have:

$$\mathrm{HSI} \vdash F = G \implies F \cong G.$$

Every derivable equation can thus be also seen as establishing a strong intuitionistic equivalence.

This correspondence between formulas and exponential polynomials suggests investigating the rules of intuitionistic proof systems as rules for transforming exponential polynomials. Let us start with the invertible rules of the intuitionistic propositional sequent calculus, LJ, written out in two columns, the left one giving a rule in formula notation, while the right one gives the same rule in exponential polynomial notation.

$$\frac{F, \Gamma \to G}{\Gamma \to (F \to G)} \qquad \frac{G^{F\Gamma}}{(G^F)^\Gamma} \tag{$\to_r$}$$

$$\frac{\Gamma \to F \quad \Gamma \to G}{\Gamma \to F \wedge G} \qquad \frac{F^\Gamma G^\Gamma}{(FG)^\Gamma} \tag{$\wedge_r$}$$

$$\frac{F, \Gamma \to H \quad G, \Gamma \to H}{(F \vee G), \Gamma \to H} \qquad \frac{H^{F\Gamma} H^{G\Gamma}}{H^{(F+G)\Gamma}} \tag{$\vee_l$}$$

The formula notation uses the identification of the usual sequent turnstile symbol "$\vdash$" and implication "$\to$" — the former is simply the top-most occurrence of the latter (implication is right-associative). The polynomial notation in addition uses the identification of the comma and "$\wedge$", up to multiset equality for "contexts", that is, up to commutativity of multiplication for polynomials corresponding to contexts.

We can thus see that the usual invertible rules of LJ correspond to polynomial simplification rules. Since these rules are either instances or compositions of high-school identities, the rules are also valid as formula-, that is, sequent isomorphisms.

The same is true for the additional invertible rules sometimes present, such as the ones of the sequent calculus G4ip [3]:

$$\frac{(F \to G \to H), \Gamma \to I}{(G \wedge F \to H), \Gamma \to I} \qquad \frac{I^{(H^G)^F \Gamma}}{I^{H^{GF}\Gamma}} \qquad (\to_l^{\wedge})$$

$$\frac{(F \to H), (G \to H), \Gamma \to I}{(F \vee G \to H), \Gamma \to I} \qquad \frac{I^{H^F H^G \Gamma}}{I^{H^{F+G}\Gamma}} \qquad (\to_l^{\vee})$$

$$\frac{F, G, \Gamma \to H}{(F \wedge G), \Gamma \to H} \qquad \frac{H^{FG\Gamma}}{H^{FG\Gamma}}. \qquad (\wedge_l)$$

In order to express a complete version of the LJ sequent calculus in terms of exponential polynomials, we need to consider the non-invertible proof rules as well. In particular, it suffices to consider the remaining rules of G4ip:

$$\frac{}{P, \Gamma \to P} \qquad \frac{}{P^{P\Gamma}} \qquad \text{(axiom)}$$

$$\frac{\Gamma \to F}{\Gamma \to F \vee G} \qquad \frac{F^{\Gamma}}{(F+G)^{\Gamma}} \qquad (\vee_r^1)$$

$$\frac{\Gamma \to G}{\Gamma \to F \vee G} \qquad \frac{G^{\Gamma}}{(F+G)^{\Gamma}} \qquad (\vee_r^2)$$

$$\frac{F, P, \Gamma \to G}{(P \to F), P, \Gamma \to G} \qquad \frac{G^{FP\Gamma}}{G^{F^P P\Gamma}} \qquad (\to_l^P)$$

$$\frac{(G \to H), \Gamma \to (F \to G) \quad H, \Gamma \to I}{((F \to G) \to H), \Gamma \to I} \qquad \frac{(G^F)^{H^G \Gamma} I^{H\Gamma}}{I^{H^{G^F}\Gamma}}, \qquad (\to_l^{\to})$$

where P denotes a prime (i.e. atomic) formula. For simplicity, we do not give a special treatment for intuitionistic absurdity, or negation; for the purpose of this paper, $\bot$ would just be an atomic proposition as any other, and $\neg$ would be replaced by implication.

Due to the absence of contraction in G4ip, all of the non-invertible rules $\frac{F}{G}$ satisfy the arithmetic inequality $F \leq G$ when variables are interpreted in $\{n \in \mathbb{N} \mid n \geq 2\}$.[1] We shall prove this in Section 3, since the case of $(\to_l^{\to})$ is not obvious.

The goal for the present section will be to derive from G4ip a proof system that will not contain any of the (bureaucratic and non-informative) invertible rules. This system, written with the help of exponential polynomial notation will be called the *high-school* variant of G4ip (HS). Proofs in HS will only consist of the translations of the informative rules of G4ip. But, please note, that the procedure for deriving HS is generic, and could be performed on another version of LJ. The advantage of working with G4ip is that the number of different non-invertible rules necessary to get a complete system is minimal.

[1]The rule $(\to_l^P)$ would have been invertible, if by invertible we only meant equivalent and not strongly equivalent (i.e. isomorphic) premise and conclusion.

The starting idea is to use the analytic transformation,

$$G^F = \mathrm{e}^{F \log G} = \exp(F \log(G)),$$

in order to decompose binary exponentiation (i.e. implication) in terms of unary exponentiation and the logarithmic function, just as the approach to normal forms in exponential fields [7].[2]

As already analyzed in a previous unpublished study of the $\beta\eta$-equations for terms of normalized type [8], the exp-log decomposition of implication leads to a normal form of propositional formulas that is obtained by left-to-right rewriting using the high-school identities (isomorphisms) (10), (11), (12), and (6).

There is some liberty in determining the order in which to apply the equations. One precise and structurally recursive procedure for computing the normal form of a formula (i.e. sequent), $\|-\|$, suitable for establishing Theorem 1, is given in Figure 1. It maps any formula to an isomorphic formula from the class of *exp-log normal forms* ($\mathcal{E}$), defined by the mutually inductively defined classes of base formulas ($\mathcal{B}$), conjunctions ($\mathcal{C}$), and disjunctions ($\mathcal{D}$):

$$\begin{aligned}
&\mathcal{B} \ni b ::= p \mid d \\
&\mathcal{C} \ni c ::= (c_1 \to b_1) \wedge \cdots \wedge (c_n \to b_n) && (n \geq 0) \\
&\mathcal{D} \ni d ::= c_1 \vee \cdots \vee c_n && (n \geq 2) \\
&\mathcal{E} \ni b ::= c \mid d,
\end{aligned}$$

that is,

$$\begin{aligned}
&\mathcal{B} \ni b ::= p \mid d && \mathcal{E} \ni b ::= c \mid d \\
&\mathcal{C} \ni c ::= \prod_{i=1}^{n \geq 0} b_i^{c_i} && \mathcal{D} \ni d ::= \sum_{i=1}^{n \geq 2} c_i,
\end{aligned}$$

where p denotes a prime formula. The variables p, c, d, e, possibly with indexing subscripts, will always be used to stand for members of the corresponding class. The unit 1 (i.e. the formula $\top$) is not a prime formula, but rather denotes the nullary product $\prod_{i=1}^{0} b_i^{c_i}$.

The formal definitions from Figure 1 are a beautified transcription of definitions carried out in the Coq proof assistant.[3] The function $\|-\|$ is defined simultaneously with the $|-|$-function, whose purpose is to guarantee the desired ordering of HSI's, i.e. that equation (6) is not applied at the base of exponentiation before equation (11). It uses the operations $\oplus$, $\times$, $\ltimes$, $\rtimes$, $\Uparrow$, and $\uparrow$. The intuition behind these operations is as follows.

The function $\oplus$ turns a binary plus (disjunction) into an n-ary one, more precisely, it flattens a tree of binary $+$-constructors into a tail-inductive list. The function $\times$ does the analogous thing for multiplication (conjunction).

[2]This hints at interpreting implication "classically", that is, in terms of two distinct "negation" symbols, $\neg_{\mathrm{exp}}$ and $\neg_{\log}$, such that

$$F \to G := \neg_{\mathrm{exp}}(F \wedge \neg_{\log} G),$$

but we do not pursue this superficial analogy further in this paper.

[3]The formalization is available at `http://github.com/dankoi/metamath/tree/master/highschool`.

$$\mathcal{B} \ni b ::= p \mid d \qquad \mathcal{C} \ni c ::= 1 \mid b^{c_1} c_2$$
$$\mathcal{D} \ni d ::= c_1 + c_2 \mid c + d \qquad \mathcal{E} \ni e ::= c \mid d$$

$$\begin{aligned} - \oplus - &: \mathcal{E} \to \mathcal{E} \to \mathcal{D} \\ c_1 \oplus e_2 &:= c_1 + e_2 \\ (c_{11} + c_{12}) \oplus e_2 &:= c_{11} + (c_{12} + e_2) \\ (c_{11} + d_{12}) \oplus e_2 &:= c_{11} + (d_{12} \oplus e_2) \end{aligned}$$

$$\begin{aligned} - \times - &: \mathcal{C} \to \mathcal{C} \to \mathcal{C} \\ 1 \times c_2 &:= c_2 \\ b^{c_{11}} c_{12} \times c_2 &:= b^{c_{11}} (c_{12} \times c_2) \end{aligned}$$

$$\begin{aligned} - \rtimes - &: \mathcal{C} \to \mathcal{E} \to \mathcal{E} \\ c_1 \rtimes c_2 &:= c_1 \times c_2 \\ c_1 \rtimes (c_{21} + c_{22}) &:= (c_1 \times c_{21}) + (c_1 \times c_{22}) \\ c_1 \rtimes (c_{21} + d_{22}) &:= (c_1 \times c_{21}) + (c_1 \rtimes d_{22}) \end{aligned}$$

$$\begin{aligned} - \uparrow - &: \mathcal{B} \to \mathcal{E} \to \mathcal{C} \\ b \uparrow c &:= b^c 1 \\ b \uparrow (c_1 + c_2) &:= (b^{c_1} 1) \times (b^{c_2} 1) \\ b \uparrow (c_1 + d_2) &:= (b^{c_1} 1) \times (b \uparrow d_2) \end{aligned}$$

$$\begin{aligned} - \Uparrow - &: \mathcal{C} \to \mathcal{E} \to \mathcal{C} \\ 1 \Uparrow e_2 &:= 1 \\ b^{c_{11}} c_{12} \Uparrow e_2 &:= (b \uparrow (c_{11} \rtimes e_2)) \times (c_{12} \Uparrow e_2) \end{aligned}$$

$$\begin{aligned} - \ltimes - &: \mathcal{E} \to \mathcal{E} \to \mathcal{E} \\ c_1 \ltimes e_2 &:= c_1 \rtimes e_2 \\ (c_{11} + c_{12}) \ltimes e_2 &:= (c_{11} \rtimes e_2) \oplus (c_{12} \rtimes e_2) \\ (c_{11} + d_{12}) \ltimes e_2 &:= (c_{11} \rtimes e_2) \oplus (d_{12} \ltimes e_2) \end{aligned}$$

$$\begin{aligned} \|-\| &: \text{Formula} \to \mathcal{E} \\ \|p\| &:= p^1 1 \\ \|F \vee G\| &:= \|F\| \oplus \|G\| \\ \|F \wedge G\| &:= \|F\| \ltimes \|G\| \\ \|F \to G\| &:= |G| \Uparrow \|F\| \end{aligned} \qquad \begin{aligned} |-| &: \text{Formula} \to \mathcal{C} \\ |p| &:= p^1 1 \\ |F \vee G| &:= (|F| \oplus |G|)^1 1 \\ |F \wedge G| &:= |F| \times |G| \\ |F \to G| &:= |G| \Uparrow \|F\| \end{aligned}$$

FIGURE 1. Formula normalization functions

The functions $\ltimes$ and $\rtimes$ apply the left, correspondingly right, distributivity law. They are meant to implement the following informal equations:

$$p \ltimes d = p^1 \rtimes d \qquad\qquad c \rtimes p = cp^1$$
$$\left(\sum_{i=1}^{n} c_i\right) \ltimes d = \sum_{i=1}^{n} (c_i \rtimes d) \qquad\qquad c \rtimes \sum_{i=1}^{n} c_i = \sum_{i=1}^{n} cc_i.$$

Finally, the functions $\Uparrow$ and $\uparrow$ normalize exponentiations following (10), (11) and (12), in order for the following informal equations to hold:

$$b \uparrow p = b^{p^1} \qquad\qquad b \Uparrow e = b \uparrow e$$
$$b \uparrow \sum_{i=1}^{n} c_i = \prod_{i=1}^{n} b^{c_i} \qquad\qquad \left(\prod_{i=1}^{n\geq 0} b_i{}^{c_i}\right) \Uparrow e = \prod_{i=1}^{n\geq 0} (b_i \uparrow (c_i \ltimes e)).$$

In order to prove Theorem 1, we shall need to establish the following lemma on *formal* equalities, where "=" denotes definitional equality modulo commutativity of multiplication.

Lemma 1. *The following equations hold for the normalization functions defined in Figure 1:*

$$c \times 1 = c \tag{13}$$
$$c_1 \times (c_2 \times c_3) = (c_1 \times c_2) \times c_3 \tag{14}$$
$$d \oplus (e_2 \oplus e_3) = (d \oplus e_2) \oplus e_3 \tag{15}$$
$$e_1 \oplus (e_2 \oplus e_3) = (e_1 \oplus e_2) \oplus e_3 \tag{16}$$
$$c \rtimes (d \oplus e) = (c \rtimes d) \oplus (c \rtimes e) \tag{17}$$
$$c \rtimes (e_1 \oplus e_2) = (c \rtimes e_1) \oplus (c \rtimes e_2) \tag{18}$$
$$(d \oplus e_1) \ltimes e_2 = (d \ltimes e_2) \oplus (e_1 \ltimes e_2) \tag{19}$$
$$(e_0 \oplus e_1) \ltimes e_2 = (e_0 \ltimes e_2) \oplus (e_1 \ltimes e_2) \tag{20}$$
$$1 \rtimes e = e \tag{21}$$
$$c_1 \rtimes (c_2 \rtimes d) = (c_1 \times c_2) \rtimes d \tag{22}$$
$$c_1 \rtimes (c_2 \rtimes e) = (c_1 \times c_2) \rtimes e \tag{23}$$
$$c \rtimes (d \ltimes e) = (c \rtimes d) \ltimes e \tag{24}$$
$$c \rtimes (e_1 \ltimes e_2) = (c \rtimes e_1) \ltimes e_2 \tag{25}$$
$$d \ltimes (e_1 \ltimes e_2) = (d \ltimes e_1) \ltimes e_2 \tag{26}$$
$$e_1 \ltimes (e_2 \ltimes e_3) = (e_1 \ltimes e_2) \ltimes e_3 \tag{27}$$
$$c \Uparrow 1 = c \tag{28}$$
$$(c_1 \times c_2) \Uparrow e = (c_1 \Uparrow e) \times (c_2 \Uparrow e) \tag{29}$$
$$b \uparrow (d \oplus e) = (b \uparrow d) \times (b \uparrow e) \tag{30}$$
$$b \uparrow (e_1 \oplus e_2) = (b \uparrow e_1) \times (b \uparrow e_2) \tag{31}$$
$$b \uparrow (e_1 \ltimes e_2) = (b \uparrow e_1) \Uparrow e_2 \tag{32}$$
$$c \Uparrow (e_1 \ltimes e_2) = (c \Uparrow e_1) \Uparrow e_2 \tag{33}$$
$$c \Uparrow (e_1 \oplus e_2) = (c \Uparrow e_1) \times (c \Uparrow e_2) \tag{34}$$
$$c \Uparrow ((e_1 \oplus e_2) \ltimes e_3) = (c \Uparrow (e_1 \ltimes e_3)) \times (c \Uparrow (e_2 \ltimes e_3)) \tag{35}$$

$$\frac{}{p \uparrow (p^1 \rtimes e)} \qquad \text{(axiom)}$$

$$\frac{c_1 \Uparrow e}{(c_1 + c_2) \uparrow e} \qquad (\vee_r^1)$$

$$\frac{c_2 \Uparrow e}{(c_1 + c_2) \uparrow e} \qquad (\vee_r^2)$$

$$\frac{c \Uparrow (\|F\| \ltimes (p \rtimes e))}{c \Uparrow ((|F| \Uparrow p) \rtimes (p \rtimes e))} \qquad (\to_l^P)$$

$$\frac{((|G| \Uparrow e_1) \Uparrow ((|H| \Uparrow \|G\|) \rtimes e_2)) \times (c \Uparrow (\|H\| \ltimes e_2))}{c \Uparrow ((|H| \Uparrow (|G| \Uparrow e_1)) \rtimes e_2)} \qquad (\to_l^{\to})$$

FIGURE 2. Proof rules of the High-school sequent calculus (HS) for G4ip

Proof. The proofs proceed as follows: (13) by induction on c; (14) by induction on c_1; (15) by induction on d; (16) by case analysis on e_1, e_2, e_3 and using (15); (17) by induction on d; (18) by case analysis on e_1, e_2 and using (17); (19) by induction on d and using (16); (20) by case analysis on e_1, e_2 and using (19); (21) by induction on e; (22) by induction on d and using (16); (23) by case analysis on e and using (22) and (16); (24) by induction on d and using (18) and (23); (25) by case analysis on e_1 and using (24) and (23); (26) by induction on d and using (20) and (25); (27) by case analysis on e_1 and using (25) and (26); (28) by induction on c and using (13); (29) by induction on c_1 and using (14); (30) by induction on d; (31) by induction on e_1 and using (30); (32) by induction on e_1 and using (13) and (31); (33) by induction on c and using (29), (32), and (25); (34) by induction on c and using (18) and (31); (35) by using (20) and (34).

It may be interesting to notice that in fact (34) is the only case that depends on the commutativity of multiplication, while the other equations have been established in Coq as definitional equalities. One can obtain a completely intensional version of the normalization function if one is willing to integrate into the definition of $\times$ a conditional expression for performing merge sort and producing results invariant over commutativity. □

Armed with a precise and terminating transformation of formulas, we can now state the HS variant of G4ip in Figure 2. Notice that our calculus consists of non-invertible rules only, tagged with the tag of the G4ip rule they correspond to (to be shown in Theorem 1 below). The rules $(\to_l^P)$ and $(\to_l^{\to})$ mention usual formulas F, G, H. This is done on purpose, so that the correspondence to G4ip rules is as tight as possible. If one wants to mention only formulas from the normalized classes, one can consider the following reformulations of the rules,

$$\frac{c \Uparrow (\partial c_0 \ltimes (p \rtimes e))}{c \Uparrow ((c_0 \Uparrow p) \rtimes (p \rtimes e))} \qquad (\to_l^{P\prime})$$

$$\frac{((c_2 \Uparrow e_1) \Uparrow ((c_1 \Uparrow \partial c_2) \rtimes e_2)) \times (c \Uparrow (\partial c_1 \ltimes e_2))}{c \Uparrow ((c_1 \Uparrow (c_2 \Uparrow e_1)) \rtimes e_2)}, \qquad (\rightarrow_l^{\rightarrow\prime})$$

where ∂ denotes the map $|F| \mapsto \|F\|$ that distributes the product over the sums of the form $(c_1 + \cdots + c_n)^1$ in $|F|$; here, the exponent 1 is used to suspend normalization, that is, permit the isomorphism (11) to be applied before (6) at the base of exponentiation.

Note also, that the normalization functions disappear from any *concrete* proof in HS notation. The functions are there merely for a compact presentation of the rules. For instance, considering the case of the $(\rightarrow_l^{\rightarrow})$-rule from HS, where $c := p^1$, $c_1 := p^1$, $c_2 := q^1$, $e_1 := r^1$, $e_2 := s^1$, and p, q, r, s are prime formulas, we retrieve just the corresponding G4ip rule in polynomial notation,

$$\frac{\left(q^{r^1 p^{q^1 1} s^1 1} 1\right)\left(p^{p^1 s^1 1} 1\right)}{p^{p^{q^{r^1 1} 1} s^1 1}},$$

or the more readable one, by a harmless abuse of notation involving 1:

$$\frac{\left(q^{r p^q s}\right)\left(p^{ps}\right)}{p^{p^{q^r} s}}.$$

For a concrete example of the rules involving disjunction, consider the case where $c_1 := p^1$, $c_2 := q^1$, $e := r^1 + s^1$, and the concrete and 1-simplified instance of the $(\vee_r^1)$ rule:

$$\frac{p^r p^s}{(p+q)^r (p+q)^s}.$$

We shall now show in which sense HS is a version of G4ip. This will also imply that HS is a proof system complete for intuitionistic provability.

Theorem 1. *Every derivation of F in G4ip can be transformed to a derivation of $\|F\|$ in HS.*

Proof. The proof is by induction on the derivation. At each case, we first apply (13) and (21) of Lemma 1 to slightly simplify the involved expressions. Then, the non-invertible rules, (axiom), $(\vee_r^1)$, $(\vee_r^2)$, $(\rightarrow_l^P)$, and $(\rightarrow_l^{\rightarrow})$, are directly proven by their HS correspondent rule. As for the invertible rules:

- $(\rightarrow_r)$ is proven by (33);
- $(\wedge_r)$ is proven by (29);
- $(\vee_l)$ is proven by (35);
- $(\rightarrow_l^{\wedge})$ is proven also by (33);
- and, $(\rightarrow_l^{\vee})$ is proven by (34).

□

Remark 1. Since $F \cong \|F\|$, the transformation of a G4ip proof into an HS one is loss-less, in the sense that it preserves the essence of the original proof modulo a given notion of identity of proofs. That is, it should not be too hard to define a reverse transformation of HS-proofs into G4ip proofs, such that the composition of the two transformations would identify G4ip proofs up to a certain equality theory on proofs. We have not done that formally, for it should be more as less clear (ex. from the two examples before the theorem, or the one that follows) that HS can be seen as a fragment of G4ip.

Although it may appear to be complex to transform G4ip proofs to HS proofs, when one wants to formally apply the normalization functions of Figure 1, this transformation is actually quite easy and can be efficiently also performed by hand using high-school arithmetic. We give an example to show how it works.

Example 1. The following G4ip derivation of $r \wedge (q \to (r \vee t) \to s) \to q \to s$,

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{s^{qrss^t}}\ \text{axiom}}{s^{qrs^r s^t}}\ (\to_l^P)}{s^{qrs^{r+t}}}\ (\to_l^\vee)}{s^{qr\left(s^{r+t}\right)^q}}\ (\to_l^P)}{\left(s^q\right)^{r\left(s^{r+t}\right)^q}}\ (\to_r)$$

is mapped to the following HS derivation:

$$\dfrac{\dfrac{\dfrac{}{s^{qrss^t}}\ \text{axiom}}{s^{qrs^r s^t}}\ (\to_l^P)}{s^{qrs^{rq} s^{tq}}}\ (\to_l^P).$$

In Section 4, we shall extend this representation of intuitionistic formulas by exponential polynomials to the first-order quantifiers.

3. The Inequality Interpretation of Inference Rules

In this section, we will show that the inference rules for G4ip can be interpreted as inequalities relating the exponential polynomials corresponding to the premises and the conclusion. This extends the previous observation that invertible rules are equalities.

We start by exploring the inequality interpretation of G4ip, in order to keep the presentation somewhat simple. The main result will be the following.

Theorem 2. *Let $\mathcal{R}$ be an inference rule of G4ip. If the variables F, G, H, I, P are interpreted to be natural numbers strictly greater than 1, then the value of the premise of the rule is less than or equal to the value of the conclusion. Moreover, the inequality is strict if and only if $\mathcal{R}$ is not invertible.*

Formally, we define an interpretation function $[\![-]\!]$ that maps formulas and contexts to natural numbers. The function is defined as follows:

$$\begin{aligned} [\![F \vee G]\!] &= [\![F]\!] + [\![G]\!] & [\![F \wedge G]\!] &= [\![F]\!] \cdot [\![G]\!] \\ [\![G \to F]\!] &= [\![F]\!]^{[\![G]\!]} & [\![\Gamma, F]\!] &= [\![\Gamma]\!] \cdot [\![F]\!] \\ [\![P]\!] &= 2 & [\![\top]\!] &= [\![\cdot]\!] = 1 \end{aligned}$$

Note that with this interpretation, we have the following property:

Lemma 2. *If $[\![F]\!] = 1$ then $F \cong \top$.*

Proof. By a straightforward induction on the structure of formulas. □

This observation justifies our assumption that when we apply an inference rule, the variables involved must have a value greater than or equal to 2. For instance,

consider the $(\to_l^{\to})$ rule. Here, we could have $F, G, H = P$, $\Gamma = \cdot$, and $I = \top$, which would result in the following interpretation:

$$\frac{(2^2)^{2^{2\cdot 1}} \cdot 1^{2\cdot 1}}{1^{2^{2^{2\cdot 1}}}}$$

Clearly, the premise does *not* have a smaller value than the conclusion, hence the inequality interpretation does not work, unless we assume all the variables (except the one corresponding to Γ) have values greater than 2.

Note, however, that this is an entirely reasonable assumption given the content of Lemma 2. If $I = \top$, there is no reason to apply the $(\to_l^{\to})$, as we already know $\top$ is provable[4]. Thus, we will assume that the formulas and contexts in question have been subjected to the following simplification rules first:

$$\begin{array}{rcl@{\qquad\qquad}rcl} \top \wedge F & \rightsquigarrow & F & F \wedge \top & \rightsquigarrow & F \\ \top \to F & \rightsquigarrow & F & F \to \top & \rightsquigarrow & \top \\ \Gamma, \top & \rightsquigarrow & \Gamma & & & \end{array}$$

These simplifications correspond to the high-school identities (7), (8), and (9). Note that we do not need to reduce occurrences of $\top$ inside disjunctions, as $[\![F \vee G]\!] \geq 2$ for all formulas F, G. This leads to the following lemma:

Lemma 3. *For all formulas F, either $[\![F]\!] \geq 2$ or $F \rightsquigarrow^* \top$.*

Proof. By induction on the structure of F. We show here a representative case. If $F = G \to H$, we apply the induction hypothesis to H. If $H \rightsquigarrow^* \top$, then $F \rightsquigarrow^* \top$ by the definition of $\rightsquigarrow$. If not, we have $[\![H]\!] \geq 2$, and thus

$$[\![G \to H]\!] = [\![H]\!]^{[\![G]\!]} \geq 2^{[\![G]\!]} \geq 2,$$

by using the fact that $[\![H]\!] \geq 2$ and $[\![G]\!] \geq 1$ respectively. □

Alternatively, one can simply replace all occurrences of $\top$ with any formula with a unique proof, such as $P \to P$ for some fresh atomic formula P.

In the rest of this section, we will omit the interpretation function, as it will be obvious from the context whether we are talking about the formula or the interpretation to which it is mapped.

Let us now return to the inference rules of G4ip. The fact that the invertible rules preserve the value of the sequents is immediate by inspection of the inference rules. For instance, for the $(\vee_l)$ rule, we would need to show that

$$H^{(F+G)\Gamma} = H^{F\Gamma} H^{G\Gamma},$$

but this is a simple arithmetical equality. This leaves the matter of establishing the non-invertible rules as strict inequalities. For the $(\vee_r^1)$ and $(\vee_r^2)$ rules, this is immediate, as $F + G > F$ and $F + G > G$ whenever $F, G \geq 1$.

For the $(\to_l^P)$ rule, we have that $F \not\cong \top$ and thus $F \geq 2$. As P is an atomic formula, its interpretation is 2, and thus

$$\begin{array}{rl} F^P = F^2 > F & \text{and hence} \\ G^{F^P P\Gamma} > G^{FP\Gamma} & \text{by monotonicity.} \end{array}$$

[4]In fact, modern presentations of G4ip omit $\top$ as a formula entirely, as it — from a proof search perspective — is completely superfluous.

This leaves the inequality associated to the $(\to_l^{\to})$ rule, for which we will need a few lemmas first:

Lemma 4. *If the inequality* $2^{H^{G^F}-H} > G^{FH^G}$ *holds for all* $G, H, F \geq 2$*, then* $I^{H^{G^F}\Gamma} > (G^F)^{H^G\Gamma} I^{H\Gamma}$ *for all* $F, G, H, I \geq 2$ *and* $\Gamma \geq 1$*.*

Proof. We reason as follows:

$$\begin{aligned}
2^{H^{G^F}-H} &> G^{FH^G} && \text{by assumption.}\\
I^{H^{G^F}-H} &> G^{FH^G} && \text{as } I \geq 2.\\
I^{(H^{G^F}-H)\Gamma} &> G^{FH^G\Gamma} && \text{by raising each side to the power } \Gamma.\\
I^{H^{G^F}\Gamma-H\Gamma} &> G^{FH^G\Gamma} && \text{by distributivity.}\\
I^{H^{G^F}\Gamma} &> G^{FH^G\Gamma} I^{H\Gamma} && \text{by multiplying with } I^{H\Gamma}.\\
I^{H^{G^F}\Gamma} &> (G^F)^{H^G\Gamma} I^{H\Gamma} && \text{by the high-school identity.}
\end{aligned}$$

□

Next, we need a few further lemmas in order to discharge the assumption in the preceding lemma:

Lemma 5. *Given* $F, H \geq 2$ *and* $G \geq 3$*, the following inequalities hold:*

$$G^F - G - 1 \geq G^{F-1} \tag{36}$$

$$2^{G^{F-1}} \geq FG \tag{37}$$

$$FH^G G \geq FH^{G-1}G + 1 \tag{38}$$

Proof. To prove (36), we reason as follows:

$$\begin{aligned}
G^{F-2} \geq G^{2-2} = G^0 = 1 && \text{as } F \geq 2.\\
3G^{F-2} - 1 > G^{F-2} && \text{as } 3n - 1 > n \text{ when } n \geq 1.\\
G^{F-1} - 1 > G^{F-2} && \text{as } G \geq 3.\\
G^F - G > G^{F-1} && \text{by multiplying with } G.\\
G^F - G \geq G^{F-1} + 1 && \text{as } G, F \in \mathbb{N}.\\
G^F - G - 1 \geq G^{F-1} && \text{by rearranging.}
\end{aligned}$$

Next, to prove (37), will do this in two steps: First, we note that the inequality holds when $F = 2$. To show this, we need to show that $2^{G^{2-1}} = 2^G \geq 2G$, that is $2^{G-1} \geq G$, which is clear when $G \geq 2$. Next, we observe that if the inequality holds for some F, then it also holds with $F + 1$ substituted in place of F. For the right hand side of the inequality, this gives a difference of $(F+1)G - FG = G$. For the left hand side, we reason as follows:

$$\begin{aligned}
2^{G^F} - 2^{G^{F-1}} &\geq 2^{G^2} - 2^{G^{2-1}} && \text{as } F \geq 2.\\
&= (2^G)^G - 2^G && \text{by the high-school identities.}\\
&\geq (2^G)^2 - 2^G && \text{as } G \geq 2.\\
&= 2^G(2^G - 1)
\end{aligned}$$

$$\geq G \qquad \text{as } 2^G \geq G \text{ and } 2^G - 1 \geq 1.$$

As we have now established that

$$2^{G^F} - 2^{G^{F-1}} \geq (F+1)G - FG$$

for all $F \geq 2$, the desired result follows from a straightforward induction on F.

Finally, to establish (38), we reason as follows:

$$\begin{aligned} FH^{G-1}G(H-1) &\geq 1 && \text{as } F, G, H \geq 2. \\ FH^G G &\geq FH^{G-1}G + 1 && \text{by rearranging.} \end{aligned}$$

□

We can now establish the final lemma:

Lemma 6. *For all $F, G, H \geq 2$, we have $2^{H^{G^F}-H} > G^{FH^G}$.*

Proof. We first prove this in the case where $G \geq 3$:

$$\begin{aligned} 2^{G^{F-1}} &\geq FG && \text{by (37).} \\ 2^{G^F - G - 1} &\geq FG && \text{as } G^F - G - 1 \geq G^{F-1} \text{ by (36).} \\ H^{G^F - G - 1} &\geq FG && \text{as } H \geq 2. \\ H^{G^F - 1} &\geq FH^G G && \text{by multiplying with } H^G. \\ H^{G^F - 1} &\geq FH^{G-1}G + 1 && \text{by (38) and transitivity.} \\ H^{G^F - 1} - 1 &\geq FH^{G-1}G \\ H^{G^F} - H &\geq FH^G G && \text{by multiplying with } H. \\ 2^{H^{G^F} - H} &\geq 2^{FH^G G} && \text{by monotonicity.} \\ 2^{H^{G^F} - H} &\geq (2^G)^{FH^G} && \text{by the high-school identity.} \\ 2^{H^{G^F} - H} &> G^{FH^G} && \text{as } 2^G > G \text{ when } G \geq 2. \end{aligned}$$

This takes care of the case when $G \geq 3$. In the case when $G = 2$, we need to show the following strict inequality:

$$2^{H^{2^F} - H} > 2^{FH^2}$$

First, we will establish the inequality

$$2^{2^F - 2} - F > 1$$

To do so, we note that it holds when $F = 2$, and all that is needed, then, is to establish that the expression $2^{2^F-2} - F$ is monotonic in F for all $F \geq 2$. Looking at successive differences, we get

$$\begin{aligned} \left(2^{2^{F+1}-2} - (F+1)\right) - \left(2^{2^F - 2} - F\right) &= 2^{2^{F+1}-2} - 2^{2^F - 2} - 1 \\ &\geq 2^{2^3 - 2} - 2^{2^2 - 2} - 1 \\ &= 2^6 - 2^2 - 1 > 0 \end{aligned}$$

whence the expression is monotonic in F. We can now complete the argument as follows:

$$\begin{aligned}
2^{2^F-2} - F > 1 &\qquad \text{by the preceding argument.}\\
H^{2^F-2} - F > 1 &\qquad \text{as } H \geq 2.\\
H(H^{2^F-2} - F) > 1 &\qquad \text{by multiplying with } H.\\
H^{2^F-1} - FH > 1 &\qquad \text{by simplification.}\\
H^{2^F-1} - 1 > FH &\qquad \text{by rearranging.}\\
H^{2^F} - H > FH^2 &\qquad \text{by multiplying with } H.\\
2^{H^{2^F}-H} > 2^{FH^2} &\qquad \text{by monotonicity.}
\end{aligned}$$

This concludes the proof. □

Combining the above lemmas, we now get Theorem 2 as a straightforward consequence.

Using this theorem, we can prove as an easy corollary that proof search using the rules of G4ip is terminating. Because none of the rules increase the value of the interpretation of sequents, and because the non-invertible rules *strictly decrease* this value, it follows that the number of non-invertible rules in a derivation is bounded by a function of the value of the goal sequent. Thus, to prove termination, it is sufficient to prove that the *invertible* rules alone are terminating, and this is a straightforward exercise.

The traditional way of showing G4ip is terminating is also done by assigning a measure to each sequent, but for this, it is sufficient to show that the measure decreases along any *branch* of the proof tree. In our presentation, we have blurred the distinction between the meta-level conjunction (i.e. multiple premises) and that of the object level, as motivated by the corresponding equations for exponential polynomials.

Finally, let us briefly remark on how to extend the above result to the HS sequent calculus. The first step is to note that the normalization functions shown in Figure 1 all preserve the value of the interpretation. Thus, all that is needed is to show that the inference rules must strictly decrease the associated values. In this case, however, the necessary inequalities are exactly the ones we established previously, and as the HS sequent calculus only has non-invertible rules, termination of proof search is immediate. Note that this again requires all occurrences of $\top$ to have been simplified away.

4. An Intuitionistic Arithmetical Hierarchy

In classical first-order logic, every formula is equivalent to a formula in prenex normal form. This is possible thanks to the classical tautologies,

$$\begin{aligned}
\forall x F \vee G &\leftrightarrow \forall x(F \vee G) && (\text{where } x \notin \mathrm{FV}(G))\\
\exists x F \wedge G &\leftrightarrow \exists x(F \wedge G) && (\text{where } x \notin \mathrm{FV}(G))\\
\forall x F \wedge G &\leftrightarrow \forall x(F \wedge G)\\
\exists x F \vee G &\leftrightarrow \exists x(F \vee G)\\
\neg\exists x F &\leftrightarrow \forall x \neg F
\end{aligned}$$

$$\neg\forall x F \leftrightarrow \exists x \neg F,$$

that allow pushing the quantifiers to the front of a formula. In intuitionistic logic, half of these rules are not valid. Nevertheless, the other half are not only equivalences but even isomorphisms. We can also write the more general:

$$\forall x F \wedge \forall x G \cong \forall x (F \wedge G) \tag{39}$$

$$\exists x F \vee \exists x G \cong \exists x (F \vee G) \tag{40}$$

$$\exists x F \to G \cong \forall x (F \to G) \qquad (\text{where } x \notin \mathrm{FV}(G)). \tag{41}$$

To see why these isomorphisms hold, it is easiest to consider a natural deduction proof system, when formal proof are terms of a suitable typed lambda calculus (see for instance the intuitionistic fragment of Table 2 from [9]) and take identity of proofs, $\equiv$, to be the standard $=_{\beta\eta}$-relation for the lambda calculus with pair types (conjunction) and sum types (disjunction). One also has terms for $\exists$-introduction ($\langle x, p\rangle$), $\exists$-elimination ($\mathrm{dest}\, p\, \mathrm{as}(x.b)\, \mathrm{in}\, q$), $\forall$-introduction ($\lambda x.p$) and $\forall$-elimination (px), and additional rules for β- and η-equality of terms for the quantifiers,

$$\begin{aligned}
(\lambda x.p)t &=_\beta p\{t/x\} \\
\mathrm{dest}\, \langle t, p\rangle\, \mathrm{as}(x.a)\, \mathrm{in}\, q &=_\beta q\{t/x\}\{p/q\} \\
p &=_\eta \lambda x.px \\
p\{q/a\} &=_\eta \mathrm{dest}\, q\, \mathrm{as}(x.b)\, \mathrm{in}\, p\{\langle x, b\rangle/a\},
\end{aligned}$$

that are analogues of the β- and η-rules concerning function types and sum types. Given this notation, for instance, the isomorphism

$$\exists x F \to G \cong \forall x (F \to G)$$

can be established using two proof terms,

$$\lambda a.\lambda x.\lambda b.a\langle x, b\rangle \tag{ϕ}$$

$$\lambda c.\lambda d.\, \mathrm{dest}\, d\, \mathrm{as}(y.e)\, \mathrm{in}\, cye, \tag{ψ}$$

by showing that $\lambda c.\phi(\psi c) =_{\beta\eta} \lambda c.c$ and $\lambda a.\psi(\phi a) =_{\beta\eta} \lambda a.a$:

$$\begin{aligned}
&(\lambda a.\lambda x.\lambda b.a\langle x, b\rangle)(\lambda d.\, \mathrm{dest}\, d\, \mathrm{as}(y.e)\, \mathrm{in}\, cye) =_\beta \\
&\qquad \lambda x.\lambda b.\, \mathrm{dest}\, \langle x, b\rangle\, \mathrm{as}(y.e)\, \mathrm{in}\, cye =_\beta \lambda x.\lambda b.cxb =_\eta c
\end{aligned}$$

$$\begin{aligned}
&(\lambda c.\lambda d.\, \mathrm{dest}\, d\, \mathrm{as}(y.e)\, \mathrm{in}\, cye)(\lambda x.\lambda b.a\langle x, b\rangle) =_\beta \\
&\qquad \lambda d.\, \mathrm{dest}\, d\, \mathrm{as}(y.e)\, \mathrm{in}\, a\langle y, e\rangle =_\eta \lambda d.(aa_0)\{d/a_0\} = \lambda d.ad =_\eta a
\end{aligned}$$

Similarly, we can show that a further formula isomorphism holds,

$$G \to \forall x F \cong \forall x (G \to F), \tag{42}$$

when $x \notin \mathrm{FV}(G)$. Namely, one can take as witnessing terms the following ones:

$$\lambda a.\lambda x.\lambda b.abx \tag{ϕ}$$

$$\lambda c.\lambda d.\lambda x.cxd. \tag{ψ}$$

Given the first-order formula isomorphisms (39), (40), (41), and (42), we shall now adopt an extended exponential polynomial notation of formulas involving quantifiers. We write $\exists x F$ as xF and $\forall x F$ as F^x, the distinction between conjunctions and existential quantifiers, and implications and universal quantifiers, being made by a variable convention: we "left-multiply" and "exponentiate" by x, y, z in order

to express quantifiers, while if we do it with F, G, it means that we are making a conjunction and implication with a generic formula. Using this notation, the isomorphisms (39)-(42) acquire the form of the following equations:

$$(FG)^x = F^x G^x \tag{39'}$$

$$x(F+G) = xF + xG \tag{40'}$$

$$G^{xF} = (G^F)^x \qquad (\text{where } x \notin \mathrm{FV}(G)) \tag{41'}$$

$$(F^x)^G = (F^G)^x \qquad (\text{where } x \notin \mathrm{FV}(G)) \tag{42'}$$

This extension of HSI with rules involving the *extended* exponential polynomials thus still implies formula isomorphism. And now we can give an interpretation of the invertible proof rules involving the quantifiers that respect this notation:

$$\frac{\Gamma \to F}{\Gamma \to \forall x F} \qquad \frac{(F^\Gamma)^x}{(F^x)^\Gamma} \qquad \text{for all } x \notin \mathrm{FV}(\Gamma) \tag{$\forall_r$}$$

$$\frac{F, \Gamma \to G}{\exists x F, \Gamma \to G} \qquad \frac{\left(G^{F\Gamma}\right)^x}{G^{xF\Gamma}} \qquad \text{for all } x \notin \mathrm{FV}(G, \Gamma). \tag{$\exists_l$}$$

As the invertible rules are equalities, an extension of HS from Section 2 for the first-order case can be defined in the same way as before, by applying a normalization function (see Figure 3) to the premises and conclusions of the non-invertible rules for quantifiers. Working with the first-order extension G4i [10] of G4ip, one would have the HS variants of the rules $(L\forall)$, $(R\exists)$, $(L\forall\supset)$, while the invertible rule $(L\exists\supset)$ can be handled using the isomorphism (41).

We have not pursued formally showing an extension of Lemma 1, mostly for technical reasons having to do with formalizing syntax with binders.[5] Hence, we do not propose to establish formally a first-order analogue of Theorem 1 here.

What we consider as a more important consequence of the extended exponential polynomial interpretation of the quantifiers is the fact that it leads to a simple normal form i.e. a simple intuitionistic "arithmetical" hierarchy that classifies intuitionistic first-order formulas up to isomorphism.

This interpretation suggests trying to obtain a normal form of first-order formulas by sometimes pushing the quantifiers *in*, rather than always pushing them out, like in the approach for classical logic. Our approach will lead to a normal form theorem which implies that a hierarchy of formulas exists for intuitionistic logic, which not only preserves strong equivalence of formulas (and hence proof identity), but is comparatively as simple as the classical arithmetical hierarchy.

Theorem 3. *For every first-order formula F, there is an isomorphic formula $e \in \Sigma \cup \Pi$, where the classes Σ, Π, and $\mathcal{B}$ are defined simultaneously as follows,*

$$\begin{aligned} &\Sigma \ni d ::= c_1 \vee \cdots \vee c_n && (n \geq 2)\\ &\Pi \ni c ::= \forall x_1(c_1 \to b_1) \wedge \cdots \wedge \forall x_n(c_n \to b_n) && (n \geq 0)\\ &\mathcal{B} \ni b ::= p \mid d \mid \exists x c, \end{aligned}$$

or, in extended exponential polynomial notation:

$$\Sigma \ni d ::= \sum_{i=1}^{n\geq 2} c_i \qquad \Pi \ni c ::= \prod_{i=1}^{n\geq 0} (b_i^{c_i})^{x_i} \qquad \mathcal{B} \ni b ::= p \mid d \mid xc,$$

[5] Apart from the fact that we do not use it for formal proofs, the Coq definition of the functions from Figure 3 is simple and can be used to compute the formula normal form.

$$\mathcal{B} \ni b ::= p \mid d \mid xc \qquad \Pi = \mathcal{C} \ni c ::= 1 \mid (b^{c_1})^{x_1} c_2$$
$$\Sigma = \mathcal{D} \ni d ::= c_1 + c_2 \mid c + d \qquad \mathcal{E} \ni e ::= c \mid d$$

$$\mathrm{Vars} \ni x ::= x_1, \ldots, x_n \mid \epsilon$$

$$\begin{aligned} - \times - &: \mathcal{C} \to \mathcal{C} \to \mathcal{C} \\ 1 \times c_2 &:= c_2 \\ (b^{c_{11}})^x\, c_{12} \times c_2 &:= (b^{c_{11}})^x\, (c_{12} \times c_2) \end{aligned}$$

$$\begin{aligned} - \uparrow^- - &: \mathcal{B} \to \mathrm{Vars} \to \mathcal{E} \to \mathcal{C} \\ b \uparrow^x ((yc)^1 1) &:= (b^c)^{x,y}\, 1 \\ b \uparrow^x c &:= (b^c)^x\, 1 \\ b \uparrow^x (c_1 + c_2) &:= ((b^{c_1})^x 1) \times ((b^{c_2})^x 1) \\ b \uparrow^x (c_1 + d_2) &:= ((b^{c_1})^x 1) \times (b \uparrow^x d_2) \end{aligned}$$

$$\begin{aligned} - \Uparrow - &: \mathcal{C} \to \mathcal{E} \to \mathcal{C} \\ 1 \Uparrow e_2 &:= 1 \\ (b^{c_{11}})^x c_{12} \Uparrow e_2 &:= (b \uparrow^x (c_{11} \rtimes e_2)) \times (c_{12} \Uparrow e_2) \end{aligned}$$

$$\begin{aligned} - \propto - &: \mathrm{Vars} \to \mathcal{E} \to \mathcal{E} \\ x \propto c &:= xc \\ x \propto (c_1 + c_2) &:= xc_1 + xc_2 \\ x \propto (c_1 + d_2) &:= xc_1 + x \propto d_2 \end{aligned}$$

$$\begin{aligned} - \Rsh^- &: \mathcal{C} \to \mathrm{Vars} \to \mathcal{C} \\ 1 \Rsh^x &:= 1 \\ ((b^{c_1})^y c_2) \Rsh^x &:= (b^{c_1})^{y,x} (c_2 \Rsh^x) \end{aligned}$$

$$\begin{aligned} \|-\| &: \mathrm{Formula} \to \mathcal{E} & \qquad |-| &: \mathrm{Formula} \to \mathcal{C} \\ \|p\| &:= p^1 1 & |p| &:= p^1 1 \\ \|F \vee G\| &:= \|F\| \oplus \|G\| & |F \vee G| &:= (|F| \oplus |G|)^1 1 \\ \|F \wedge G\| &:= \|F\| \ltimes \|G\| & |F \wedge G| &:= |F| \times |G| \\ \|F \to G\| &:= |G| \Uparrow \|F\| & |F \to G| &:= |G| \Uparrow \|F\| \\ \|\exists x F\| &:= x \propto \|F\| & |\exists x F| &:= x\, |F| \\ \|\forall x F\| &:= |F| \Rsh^x & |\forall x F| &:= |F| \Rsh^x \end{aligned}$$

FIGURE 3. Extension of Figure 1 for the quantifiers

where p denotes a prime formula, and x a (potentially empty) list of first-order variables.

Proof. The implementation in Figure 3 is structurally recursive, hence terminating, and with range $\Sigma \cup \Pi$. □

As we mentioned, unlike the classical hierarchy that always pushes out the quantifiers – proceeding on (half of) the same equations – the proposed intuitionistic hierarchy partly pushes them in ((39) and (40)) and partly pushes them out ((41) and (42)).

Also, while the classical hierarchy proceeds in levels $\Sigma^0_n \,/ \Pi^0_n$ along a linear order for n, for our hierarchy, it is not clear whether one can define such an order; the level of a formula in Π would depend both on the level of its subformula in Π and on the level of its subformula in $\mathcal{B}$.

5. Conclusion

The reduction of logic to high-school arithmetic is the general contribution of this paper. Such a reduction is not in itself a new idea, present ever since Gödel's *Dialectica* interpretation of intuitionistic logic for extracting computational content from proofs. However, in this paper we employ it to study the structure of proofs and formula equivalence, allowing a fresh perspective on intuitionistic proof theory and a first link to other areas of computer science and mathematics, which one could potentially exploit to obtain new results in Logic.

Indeed, as we saw, seeing proof rules as relations (inequalities) between exponential polynomials allowed us to define HS. As far as we know, this is the first proof formalism for intuitionistic logic that dispenses with invertible proof rules. We thus believe it to be a fresh contribution to the study of identity of proofs [1], an open problem identified already by Kreisel [11] and Prawitz [12]. Proving that HS-notation alone is enough to define identity of proofs is a topic of future work. In a related unpublished work [8], we have studied the equational theory of $=_{\beta\eta}$ for the lambda calculus with sum types (i.e. intuitionistic natural deduction), after terms are coerced to a type normal form similar to the one shown in Figure 1. A new decomposition of $=_{\beta\eta}$ is proposed there, from which one can also see that the permutations of invertible rules are an obstacle for comparing derivations, and that a natural deduction calculus is less suitable than a sequent calculus for studying proof identities.

The idea that invertible proof rules of sequent calculus should be treated in blocks, inside which the order of application of rules does not matter, is present in the approach to *focused sequent calculi* such as Liang and Miller's intuitionistic system LJF [2], inspired by previous work on linear logic by Andreoli [13]. The difference between our approach and LJF is that working on the top-most connectives of a sequent (formula) does not allow one to apply all applicable type isomorphisms as sequent transformations, and, as a consequence, a focusing proof proceeds in an alternation of invertible and non-invertible blocks of proof rules – the invertible rules still being present.

As we have shown, all the rules of the HS calculus are interpreted as strict inequalities of natural numbers when atoms are instantiated with appropriately chosen values. Because our exponential polynomials are manifestly monotonic when interpreted as functions (i.e. if $f(x)$ is an exponential polynomial containing the

variable x, and $n \leq m$, then $f(n) \leq f(m)$), one might consider allowing the application of the inference rules in Figure 2 not only at the top level of the sequent, but also *deeply* inside the formulas themselves. This could lead to a *deep inference* [14] calculus in the style of G4ip. Moreover, because of the aforementioned monotonicity, it should be possible to extend the results of Section 3 to ensure that this calculus is terminating as well. Note that intuitionistic calculi presented as deep inference systems (see e.g. [15]) usually have an explicit contraction rule, which precludes such a termination argument.

Compared to more traditional sequent calculi, HS is maybe closer to Vorob'ev's original calculus [16], that contains distributivity proof rules (i.e. (6)), than Dyckhoff's [3] and Hudelmaier's [17], which do not apply such proof rules.

Furthermore, we showed that the inequality interpretation allows us to formulate a simple termination argument for proof search in intuitionistic propositional logic. This could be potentially useful for automated and inductive theorem proving.

Finally, the formula hierarchy from Section 4 appears to be the first systematic classification of first-order formulas up to isomorphism. One could also argue that it is the simplest hierarchy for intuitionistic logic so far and reminiscent of the classical arithmetical hierarchy. Our hierarchy could also be used as an alternative one in the context of classical logic, for the cases where the desirable equivalence of formulas is not the classical one but isomorphism, however, it is not clear at this moment whether there is a meaningful (non-degenerated) notion of proof identity for classical proof systems.

Previous intuitionistic hierarchies that we know of are the ones of Mints [18], Leivant [19], Burr [20], and Fleischmann [21]. Mints' classification of formulas is restricted to ones not containing negative occurrences of quantifiers, with the aim of showing complexity bounds on termination of proof search; this line of work has recently been continued by Schubert, Urzyczyn, and Zdanowski [22]. Leivant defined formula classes for intuitionistic logic based on implicational complexity, that is the depth of negative nestings of implications. Burr proposes a formula class Φ_n, that over classical logic coincides with the class Π^0_1 of the arithmetical hierarchy, however he gives no "reasonable counterpart" for the classes Σ^0_n when $n \geq 2$. Fleischmann introduces inductive operators for universal, $\mathcal{U}(\cdot,\cdot)$, and existential, $\mathcal{E}(\cdot)$, closure of sets of formulas, showing they can be used to obtain a number of different hierarchies, one of them coinciding with Burr's hierarchy, and then uses these operators to obtain model theoretic preservation theorems. It is not clear how to obtain our hierarchy using Fleischmann's operators, in the form in which they are given; also, our hierarchy classifies formulas modulo isomorphism, not only modulo equivalence.

It might also be interesting to notice a connection with the class of coherent or geometric formulas [23]: using our notation, they can be written in the form $(x_1c_1 + \cdots + x_nc_n)^{p_1 \cdots p_m} \in \mathcal{C}$. Whether any of the characteristic properties of geometric formulas can be generalized to work on formulas in our normal form, remains to be seen.

Acknowledgement. This work has been funded by ERC Advanced Grant ProofCert and has benefited from discussions with our colleagues Zakaria Chihani, Anupam Das, Nicolas Guenot, and Dale Miller.

References

[1] Kosta Došen. Identity of proofs based on normalization and generality. *Bulletin of Symbolic Logic*, 9(4):477–503, 2003.

[2] Chuck Liang and Dale Miller. Focusing and polarization in intuitionistic logic. In Jacques Duparc and Thomas A. Henzinger, editors, *Computer Science Logic*, volume 4646 of *Lecture Notes in Computer Science*, pages 451–465. Springer Berlin Heidelberg, 2007.

[3] Roy Dyckhoff. Contraction-free sequent calculi for intuitionistic logic. *The Journal of Symbolic Logic*, 57(3), 1992.

[4] Marcelo Fiore, Roberto Di Cosmo, and Vincent Balat. Remarks on isomorphisms in typed lambda calculi with empty and sum types. *Annals of Pure and Applied Logic*, 141(1–2):35 – 50, 2006.

[5] Stanley N. Burris and Karen A. Yeats. The saga of the high school identities. *Algebra Universalis*, 52:325–342, 2004.

[6] Danko Ilik. Axioms and decidability for type isomorphism in the presence of sums. In *Proceedings of the Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, CSL-LICS '14, pages 53:1–53:7, New York, NY, USA, 2014. ACM.

[7] Godfrey Harold Hardy. *Orders of Infinity. The 'Infinitärcalcül' of Paul Du Bois-Reymond*. Cambridge Tracts in Mathematics and Mathematical Physics. Cambridge University Press, 1910.

[8] Danko Ilik. A compact representation of terms and extensional equality at the exp-log normal form of types. Manuscript, arXiv:1502.04634, 2015.

[9] Danko Ilik. Delimited control operators prove double-negation shift. *Annals of Pure and Applied Logic*, 163(11):1549 – 1559, 2012.

[10] Roy Dyckhoff and Sara Negri. Admissibility of structural rules for contraction-free systems of intuitionistic logic. *Journal of Symbolic Logic*, 65:1499–1518, December 2000.

[11] G. Kreisel. A survey of proof theory II. In J.E. Fenstad, editor, *Proceedings of the Second Scandinavian Logic Symposium*, volume 63 of *Studies in Logic and the Foundations of Mathematics*, pages 109 – 170. Elsevier, 1971.

[12] Dag Prawitz. Ideas and results in proof theory. In J.E. Fenstad, editor, *Proceedings of the Second Scandinavian Logic Symposium*, volume 63 of *Studies in Logic and the Foundations of Mathematics*, pages 235 – 307. Elsevier, 1971.

[13] Jean-Marc Andreoli. Logic programming with focusing proofs in linear logic. *Journal of Logic and Computation*, 2:297–347, 1992.

[14] Alessio Guglielmi. A system of interaction and structure. *ACM Trans. Comput. Logic*, 8(1), January 2007.

[15] Nicolas Guenot and Lutz Straßburger. Symmetric normalisation for intuitionistic logic. In *Proceedings of the Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, CSL-LICS '14, pages 45:1–45:10, New York, NY, USA, 2014. ACM.

[16] N. N. Vorob'ev. A new algorithm of derivability in a constructive calculus of statements. *Trudy Matematicheskogo Instituta imeni V. A. Steklova*, 52:193–225, 1958.

[17] Jörg Hudelmaier. An O(n log n)-space decision procedure for intuitionistic propositional logic. *Journal of Logic and Computation*, 3(1):63–75, 1993.

[18] Grigorii Efroimovich Mints. Solvability of the problem of deducibility in LJ for a class of formulas which do not contain negative occurrences of quantors. *Proceedings of the Steklov Institute of Mathematics*, 98:135–145, 1968.

[19] Daniel Leivant. Implicational complexity in intuitionistic arithmetic. *The Journal of Symbolic Logic*, 46(2), 1981.

[20] Wolfgang Burr. Fragments of Heyting arithmetic. *The Journal of Symbolic Logic*, 65(3):1223–1240, 2000.

[21] Jonathan Fleischmann. Syntactic preservation theorems for intuitionistic predicate logic. *Notre Dame Journal of Formal Logic*, 51(2), 2010.

[22] Aleksy Schubert, Paweł Urzyczyn, and Konrad Zdanowski. On the Mints hierarchy in first-order intuitionistic logic. In Andrew Pitts, editor, *Foundations of Software Science and Computation Structures*, volume 9034 of *Lecture Notes in Computer Science*, pages 451–465. Springer Berlin Heidelberg, 2015.

[23] Marc Bezem and Thierry Coquand. Automating coherent logic. In Geoff Sutcliffe and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning*, volume 3835 of *Lecture Notes in Computer Science*, pages 246–260. Springer Berlin Heidelberg, 2005.